Comptroller of the Currency
Administrator of National Banks

Internal Control

Comptroller's Handbook

August 1998

M

Management

Internal Control Table of Contents

Introduction 1
- Background 1
- Internal Control Objectives 2
- Internal Control Systems 3
- Board and Senior Management Responsibility 5
- Evaluating Internal Control 6

Examination Procedures 12
- General Procedures 12
- Quantity of Risk 14
- Quality of Risk Management 15
- Conclusions 23

Appendix 25
- A. Statutory and Regulatory Requirements 25

References 27

Background

Effective internal control is essential to a bank's management of risk. Indeed, it is the foundation of safe and sound banking. When properly designed and consistently enforced, a good system of internal controls will help management safeguard the bank's resources, produce reliable financial reports, and comply with laws and regulations. It will also reduce the possibility of significant errors and irregularities, as well as assist in their timely detection when they do occur.

The OCC's evaluation of each national bank's internal controls is requisite to proper supervision of the national banking system. Bankers and examiners should both know the following guidelines governing national banks' internal control:

- The board of directors and senior management cannot delegate their responsibilities for establishing, maintaining, and operating an effective system of internal control.
- Bankers and examiners must each verify the integrity of internal control systems.
- The OCC will perform an internal control assessment during every regular on-site examination using minimum core assessment standards.

The hallmark of a positive control environment is a commitment by the board of directors and senior management to strong controls. Management and the board make sure that the bank's information systems produce pertinent and timely information in a form that enables employees and examiners to carry out their responsibilities. Bank personnel are competent and ethical. Management assigns authority and responsibility with a view to controls. And the board and its committees, especially the audit and risk management committees, pay considerable attention to whether controls are working properly.

The procedures in this booklet facilitate examiner conclusions about a bank's internal control environment. This booklet supplements the OCC's "core assessment" standards in the "Large Bank Supervision" and the "Community Bank Supervision" booklets of the *Comptroller's Handbook.* The core assessment standards require examiners to review the internal control environment during every 12- or 18-month supervisory cycle. Further guidance on assessing controls can be found in *Comptroller's Handbook* booklets on specific banking products and activities. Examiners should consult as many of these references as necessary.

Internal controls must be well understood and consistently applied. Only then can board and management policies be carried out as planned. Controls typically (1) limit authorities, (2) safeguard access to and use of records, (3) separate and rotate duties, and (4) ensure both regular and unscheduled reviews, including testing.

The federal banking agencies have established operational and managerial standards for internal control and information systems (see 12 CFR 30, Safety and Soundness Standards, and appendix A of this booklet, "Statutory and Regulatory Requirements"). A bank should maintain a system of internal controls appropriate to its size and the nature, scope, and risks of its activities. Failure to do so may be inconsistent with established safety and soundness standards, possibly subjecting the bank to supervisory action.

Although internal control and internal audit are closely related, internal and external audits are the topics of a different section of the *Comptroller's Handbook.* That section addresses how bank audit programs help bank directors and management monitor and control risks.

Internal Control Objectives

An effective control system helps to ensure

- Efficient and effective bank operations.
- The accuracy and integrity of recorded transactions.
- The reliability of financial reporting.
- An effective risk management system.
- Compliance with banking laws and regulations, as well as internal policies and procedures.

Control systems can help bank managers measure performance, make decisions, evaluate processes, and limit risks.

A good internal control system can help a bank achieve its objectives and avoid surprises. Although mistakes because of personal distraction, carelessness, fatigue, errors in judgment, or misunderstanding of instructions can occur despite the control system, the better control systems minimize such mistakes.

For more discussion on the evaluation of internal control as part of the risk assessment process, refer to the "Large Bank Supervision" and the "Community Bank Supervision" booklets of the *Comptroller's Handbook*,

OCC Bulletin 96-39 "Data Communications Networks – Risks and Control Systems," and the *Federal Financial Institutions Examination Council Information Systems Examination Handbook*.

Internal Control Systems

The OCC does not endorse any specific internal control system. The formality of any control system will depend largely on a bank's size and the complexity of its operations. Internal control systems at community banks can be as effective as those at large banks, even though they are likely to be less formal and structured. But according to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), every effective control system will have:

- A control environment.
- Risk assessment.
- Control activities.
- Accounting, information, and communication systems.
- Self-assessment or monitoring.

The **control environment** reflects the board of directors' and management's commitment to internal controls. It provides discipline and structure to the control system. Elements of the control environment include:

- The integrity, ethics, and competence of personnel.
- The organizational structure of the bank.
- Management's philosophy and operating style.
- Various external influences that affect a bank's operations and practices, such as independent audits.
- How authority and responsibility are assigned, and how people are organized and developed (e.g., personnel policies and practices).
- The attention and direction provided by the board of directors and its committees, especially the audit committee and risk management committee.

Risk assessment is the identification and analysis of risks, both internal and external. Risks must be assessed because they can prevent the bank from reaching its objectives or can jeopardize its operations. An assessment helps determine what the risks are, how they should be managed, and what controls are needed.

Control activities are the policies, procedures, and practices established to help ensure that bank personnel carry out board and management directives. These activities also help ensure that the board and management act to control risks that could prevent a bank from attaining its objectives. Control activities take place throughout a bank. They should include:

- Reviews of operating performance.
- Approvals and authorization for transactions and activities.
- Segregation of duties to reduce a person's opportunity to commit and conceal crimes or errors. For example, assets should not be in the custody of the person who authorizes and records transactions.
- Requiring officers and employees in sensitive positions to be absent for two consecutive weeks each year.
- Design and use of documents and records to help ensure that transactions and events are recorded. For example, using pre-numbered documents facilitates monitoring.
- Safeguarding access to and use of assets and records. To safeguard data processing areas, for example, a bank could secure facilities and control access to computer programs and data files.
- Independent checks on whether certain jobs are getting done and certain recorded amounts are accurate. Some examples are reconciliations, computer-programmed controls, management review of reports that summarize account balances, and user review of computer-generated reports.

Although the OCC encourages banks to have written internal control procedures, having them is not enough. Personnel must understand them well and follow them conscientiously. Banks are required by regulation or policy to develop written procedures or controls on certain subjects, including insider transactions, Bank Secrecy Act, Bank Bribery Statute, real estate lending, asset management, and emerging market and trading activities.

Accounting, information, and communication systems capture and impart pertinent and timely information in a form that enables employees to carry out their responsibilities. Accounting systems are the methods and records that identify, assemble, analyze, classify, record, and report a bank's transactions. Information and communication systems enable all personnel to understand their roles in the control system, how their roles relate to others, and their accountability. Information systems produce reports on

operations, finance, and compliance that enable management and the board to run the bank. Communication systems impart information throughout the bank and to external parties such as regulators, examiners, shareholders, and customers.

Self-assessment or monitoring is the bank's own oversight of the control system's performance. Self-assessments are periodic discrete evaluations of a department's or operation's controls by the person responsible for the area; ongoing monitoring is carried out during the normal course of operations and performance of duties. Some banks use a combination of ongoing monitoring and discrete evaluations. Internal and external audits can provide independent assessments of the quality and effectiveness of a control system's design and performance. All bank personnel should share responsibility for self-assessment or monitoring; everyone should understand his or her responsibility to report any breaches of the control system.

Qualified personnel, effective risk identification and analysis, clear designation and appropriate separation of responsibilities, accurate and timely information flow, and established monitoring and follow-up processes are typical of strong control cultures. For example, in the lending area, banks with an effective internal control environment have: a board of directors active in approving and monitoring loan policies and practices; a loan review function that evaluates the risk and quality of loan portfolios; policies and procedures governing, among other items, types of loans, loan approvals, maturity limits, rate structure, and collateral requirements; and information systems that allow for proper management of the lending area.

Board and Senior Management Responsibility

A bank's board of directors and management are responsible for establishing and maintaining an effective internal control system. They ensure that the system operates as intended and that it is modified appropriately when circumstances dictate. They also ensure that it meets statutory and regulatory requirements (see appendix A of 12 CFR 30, Operational and Managerial Standards, as well as appendix A of this booklet).

The board of directors, which oversees the control system in general, approves the policies that govern the system. Management, which oversees operations, provides leadership and direction for the communication and monitoring of control policies, practices, and processes. Internal auditors, who evaluate the effectiveness of control systems, often have a significant monitoring role.

Bankers and examiners must consider whether a control system's methods, records, and procedures are proper in relation to the bank's:

- Size.
- Organization and ownership characteristics.
- Business activities.
- Operational complexity.
- Risk profile.
- Methods of processing data.
- Legal and regulatory requirements.

The proliferation of emerging technologies, enhanced information systems, and electronic banking has created new risk and control issues for banks and their regulators. These issues include: more users with access to information systems; less segregated duties; a shift from paper to electronic audit trails; a lack of standards and controls for end-user systems; and more complex contingency planning and recovery planning for information systems. The board of directors and examiners must ensure that management properly considers the risks of emerging technologies.

Evaluating Internal Control

Good internal controls are the backbone of a bank's risk management system. With that fact in mind, examiners evaluate internal controls and the policies, procedures, practices, and personnel that make them work. To evaluate internal controls in any area, examiners must understand the area's procedures and practices. Information on these subjects will come to light when examiners perform examination procedures for each area. How thoroughly an examiner must verify controls depends on the level of supervisory concern with the area and the direction of risk in the area. Examiners verify by inquiring, observing, and testing.

Verification (or validation) is the process of independently testing the integrity of control systems. Examiners should ensure that all control systems are validated according to the following cycles: In large banks, examiners validate control systems annually for high-risk areas, and once every three years for low-risk areas. In community banks, examiners validate controls every supervisory cycle to meet the core assessment standards. In any bank, examiners decide whether to seek validation beyond that required by the standards.

Scope and Objectives

The scope, type, and depth of an examiner's review of a bank's internal control depend on the size of the bank, the complexity of its operations, and its risk profile. The review should be based on the supervisory strategy for the bank, specifically on the strategic objectives. The review should focus on the nine categories of risk as defined by the OCC's risk assessment system.

If warranted, examiners should expand their review to specific banking activities or products.

To evaluate the overall adequacy of controls, the examiner should review the bank's operating systems and procedures by consulting all available sources of information, including bank personnel. Useful sources of information might include organization charts, procedural manuals, operating instructions, job specifications and descriptions, directives to employees, flow charts, and internal and external audit material.

Examination of Internal Controls

The examination procedures in this booklet enable an examiner to reach a general conclusion about a bank's control environment. This conclusion can derive from a number of assessments of individual activities or from a general evaluation. The procedures focus on essential internal controls, and they are the basis for the minimum core assessment standards for internal control in the "Large Bank Supervision" and "Community Bank Supervision" booklets of the *Comptroller's Handbook*.

Examiners must complete the core assessment during an institution's supervisory cycle. Examiners may supplement the procedures in the core assessment with the more detailed optional procedures in this booklet. The procedures in other *Comptroller's Handbook* booklets on specific banking activities may also be used. Examiners should use judgment to decide when to use the more detailed optional procedures; among their considerations should be the condition of the bank, the quantity of risk, the quality of risk management, and the background and experience of the examination team.

The internal control procedures outlined in this and other booklets closely follow the COSO standards. The procedures are structured to ensure that, at a **minimum**, examiners conclude whether the quality of risk management in the following areas is *strong, satisfactory, or weak*:

- The overall system of internal controls.
- The control environment.
- The risk assessment process.
- Control activities.
- Accounting, information, and communication.
- Self-assessment and monitoring.

Examiners must also determine what effect any undue risk posed by a bank's internal control environment may have on the bank's capital and earnings.

OCC's internal control examination procedures are organized to ensure a logical work flow. For example, after each minimum conclusion, one or more objectives are listed that precisely define how an examiner reaches the conclusion. An examiner achieves objectives by performing the optional procedures that follow the objectives.

Considerations in the Examiner's Review

In reviewing the internal controls in a specific area of the bank, an examiner should identify the key positions. For each key position, the examiner should ask:

- Is this a critical position? That is, can a person in this position make a significant error that will result in the inaccurate recording of transactions? Can he or she enter false information or gain control of assets?

- If an error or irregularity occurs, would normal routines promptly disclose it? That is, what controls exist that would prevent or detect significant errors or irregularities?

- Is it possible for a person to conceal an error or irregularity, and are there controls in place to minimize this possibility?

The examiner should primarily be concerned with positions having influence over financial records and access to assets. Persons in these positions could be involved in information processing (computer programmers) or investment and trading activities (traders, buyers, sellers). Any control system can be abused, whether computerized or manual. Once key positions have been identified, the examiner must determine which positions have the opportunity to conceal an error or irregularity. The question is not whether an individual is honest but whether internal controls will either prevent errors and irregularities or uncover them promptly. One example of such controls is the requirement that employees in key or influential positions be absent two consecutive weeks each year.

Examiners should ensure that duties and responsibilities are properly segregated to prevent errors and irregularities. In the investment area, the following duties should be strictly segregated: executing securities transactions, approving transactions, having access to securities, and posting or reconciling related accounting records. Examiners should investigate any activity in which proper controls would prevent persons having custody of assets from keeping the records. The segregation of duties can break down when this control does not keep pace with a bank's growth and diversification, practices become lax, or personnel use their knowledge or influence to circumvent this control.

Before reaching conclusions about a specific area's internal control, examiners must consider certain accounting or administrative issues. The examiner must be alert to circumstances that may cause bank employees or officers to take undue risks. The examiner should be especially alert to circumstances in which the personal financial interests of key officers or employees depend directly on the financial condition of the bank. Sound internal control ensures that conflicts of interest are minimized or controlled. Manifest or potential conflicts of interest should be incorporated in the overall assessment of the adequacy of internal control. For additional information in this area, please refer to the "Insider Activities" booklet of the *Comptroller's Handbook*.

In addition, the examiner should be alert for deviations by bank personnel from established policies, practices, and procedures. Such deviations may exist when:

- Instructions and directives are not reviewed and revised regularly to reflect current practices.
- Employees use shortcuts to perform their tasks, circumventing internal control procedures.
- Changes in organization or activities are not reflected in policies or procedures.
- Employees' duties are changed significantly in ways that may affect internal control policies.

Those and other circumstances may modify established bank procedures to such a degree that the examiner cannot properly evaluate certain internal controls until the practices are redefined. Examining personnel should report deviations, along with an assessment of their significance, to the examiner-in-charge (EIC).

The proliferation of computer systems and personal computers (PCs) requires increased controls over computer operations. Because banks rely so much on computers, embezzlement or misuse of funds is often a computer crime. The list of persons whose computers give them access to assets or financial records is long; it includes computer operators, programmers, their supervisors, and others. Banks should impose sophisticated controls not only on mainframe operations but also on the systems and records maintained on PCs, local area networks (LANs), and wide area networks (WANs). Controls on these systems are of paramount importance; refer to the *Federal Financial Institutions Examination Council Information System Examination Handbook* for further details on such controls.

Controls over information processing should be adequate to ensure the integrity of management information systems, books, and records. For example, pertinent information should be entered into processing systems in a timely manner and independently tested for accuracy. Trial balances and subsidiary ledgers should be maintained and reconciled to general ledgers in a timely manner. Differences noted should be investigated and resolved, and completed reconcilements should be reviewed and approved by appropriate personnel in a timely manner.

Conclusions

Examiners should give the EIC written, narrative comments on significant findings, both positive and negative, about the control system. The EIC uses these findings to determine how the quality of the control system affects the bank's risk management system. (In the long run, internal control findings and comments also help examiners establish and maintain a core knowledge base of a bank.)

A significant deficiency in a control system is a deficiency in risk management. For example, the failure to process transactions in an accurate, thorough, and timely manner (a failure of internal control) exposes the bank to potential losses (transaction risk). Moreover, such failures may lead to compliance errors, employee fraud, inaccurate management information systems, and material misstatements in financial statements.

Examiners should document fully specific weaknesses, as well as recommendations on how to correct them. Doing so facilitates their review and their incorporation in the report of examination. The EIC should discuss significant weaknesses or recommendations with bank management. Serious weaknesses should be communicated directly to the board of directors or audit committee. For banks with serious weaknesses, examiners should discuss whether to recommend that the bank adopt a compliance plan, per 12 CFR 30, tailored to its size and the nature, scope, and risk of its activities. A memorandum summarizing this discussion should be filed in the examination working papers. The appropriate OCC supervisory office determines whether a compliance plan is required, as it does for all corrective actions. That decision turns on how grave are the bank's control weaknesses, how broad-based is its noncompliance with operational and managerial standards, and how much these problems jeopardize the bank's safety and soundness.

Documentation of Controls

Examiners should reference and file supporting documentation in examination working papers according to OCC working paper guidelines (PPM 5400-8, "Examination Working Papers"). Although narrative

descriptions can often adequately explain an internal control system, the examiner should consider using flow charts or other diagrams. Flow charts transform complex circumstances into an easily understandable sequence of steps. Examiners should reproduce or excerpt any readily available information, such as system flow charts or job procedure descriptions, and incorporate the information in the examination working papers to avoid duplication of effort.

General Procedures

These procedures will help an examiner to determine whether the bank's policies, procedures, and processes are adequate with respect to internal control functions. Evaluating a bank's internal control functions involves assessing control functions and processes of the whole bank, as well as specific bank activities. Examiners reviewing internal control should closely coordinate their activities with those of examiners responsible for other areas of the bank. Doing so can reduce burden on the bank and keep examiners from duplicating their efforts. Sharing examination data also can be an effective cross check on the integrity of the bank's compliance and processes. The examiner's assessment of risk and the examination scope memorandum should determine how much testing and which procedures are necessary to meet examination objectives. Examiners are seldom required to follow every procedure.

Objective: Determine the scope of the examination of internal control.

1. Obtain and review the following documents to identify any previous problems that require follow-up:

   - ☐ Supervisory strategy in the OCC database.
   - ☐ EIC's scope memorandum.
   - ☐ Previous report of examination and OCC database overall summary comments.
   - ☐ Internal and external audit reports, including any management assertions and independent public accountant attestations on internal controls.
   - ☐ Minutes of any audit committees, and applicable board of director minutes since the last examination.
   - ☐ Correspondence memorandum.

2. Determine during early discussion with management:

   - How management supervises internal control activities.
   - Any material changes in the internal control functions.
   - Any internal or external factors that could affect or have affected the internal control function.

3. Determine that all significant internal control deficiencies noted in audit reports have been corrected or determine the reason why corrective action has not been initiated by:

   - Distributing to each examiner assigned an examination area a copy of significant internal control deficiencies for that area.

   - Requesting that the examiner prepare and return a memorandum regarding actions taken by the board or management to address the internal control deficiencies.

   - Assessing management's ability and desire to implement corrective action.

4. Consult with the EIC to determine whether direct testing or validation of any of the internal control programs is to be performed. If so, coordinate with the examiner performing that work program and:

   - Provide the examiner with the audit report for the specific area to be tested.

   - Make sure audit work papers are available for review.

5. Based on what was learned from these procedures and discussions with the bank EIC, determine the scope of this examination and its objectives.

Quantity of Risk

Conclusion: **The quantity of risk is (low, moderate, high).**

Objective: Determine whether the internal control environment poses undue risk to the institution's earnings and capital.

1. Determine the magnitude of control exceptions.

2. Evaluate the strength of the internal control environment.

   Consider:

   - Adequacy of staffing levels.
   - Strength of management.

3. Evaluate the actual or potential effect of control deficiencies upon the financial performance of the institution.

   Consider:

   - Financial effect of inaccurate, untimely, or improper transactions.
   - Previous losses from fraud.
   - Claims against insurance policies.
   - Employee turnover.
   - Other high operational losses.

Quality of Risk Management

Conclusion: **The quality of risk management, as reflected in the overall system of internal controls, is (strong, satisfactory, weak).**

Control Environment

Conclusion: The control environment is (strong, satisfactory, weak).

Objective: Determine whether the institution's culture embodies the principles of strong internal controls.

1. Assess the effectiveness of the control environment.

   Consider:

   - The integrity, ethics, and competence of personnel.
   - The organizational structure of the institution.
   - Management's philosophy and operating style (i.e., strategic philosophy).
   - External influences affecting operations and practices (e.g., independent audits).
   - Methods of assigning authority and responsibility, and organizing and developing people (e.g., personnel policies and practices).
   - The attention and direction provided by the board of directors and its committees, especially the audit or risk management committees.

2. Determine whether policies regarding the importance of internal control and appropriate conduct are communicated to all employees.

   - Are the policies communicated appropriately to all employees?
   - Do codes of conduct or ethics policies exist?

3. Determine whether a process has been established to monitor compliance with internal control procedures or codes of conduct.

   - Do audit or other control systems exist to periodically test for compliance with policy?

- Do audit or other control system personnel routinely review policies and training regarding ethics or codes of conduct?

Risk Assessment

Conclusion: The risk assessment process is (strong, satisfactory, weak).

Objective: Determine whether the institution's system of internal controls is appropriate for the type and level of risks undertaken by the institution's activities.

1. Assess management's ability to plan for and respond to existing and emerging risk areas.

   Consider:

   - Whether control issues are discussed and appropriately considered during the pre-planning stages for new products.
   - Whether audit personnel or other internal control experts are involved when the bank is developing new products and activities.
   - Whether audit personnel or other internal control experts are involved in the risk assessment and evaluation process.
   - Whether technology issues are considered and appropriately addressed.

2. Determine whether the bank has the appropriate operational tools to safeguard assets and ensure the integrity of accounting data/financial reports.

   Consider whether the system of internal controls includes:

   - Policies approved by the board of directors.
   - Directives or procedures endorsed by management.
   - Sufficient staff members who are competent and knowledgeable and who have adequate resources.
   - A system of checks and balances.

Control Activities

Conclusion: Control activities are (strong, satisfactory, weak).

Objective: Determine whether the board and senior management have established policies, procedures, practices, or limits.

1. Assess the effectiveness of control activities in all lines of business.

   Consider whether:

   - Policies and procedures exist to ensure that critical decisions are made with appropriate approval.
   - Processes exist to ensure independent verification of an appropriate sample of transactions to ensure integrity.
   - Processes exist to ensure ongoing and independent reconciliations of balances, both on- and off-balance-sheet.
   - Key risk-taking activities are appropriately segregated from reconciliation activities.
   - Processes exist to ensure policy overrides are minimal and exceptions are reported to management.
   - Systems exist to ensure critical employees do not have absolute control over given areas. For example:
     - Does a vacation policy for critical employees exist which ensures their absence for at least a two-week period?
     - Is there a system in place to ensure that duties are rotated periodically?

2. Determine whether reporting lines provide sufficient independence of the control function from the business line.

   - Is separation of duties emphasized in the organizational structure?
   - Are systems in place to ensure that personnel abide by separations of duty?

3. Determine whether operating practices conflict with established areas of responsibility and control.

Consider:

- Interviews with line and management personnel.
- Review of policies delineating responsibilities.
- Review of reconciliations and transaction originations.
- Review of internal audit working papers.
- Review of external audit reports.

4. Determine whether internal audit or alternate control reviews are sufficiently independent.

   Consider:

   - Where the function is located, administratively, within the organization.

   - To whom, or to what level, the function reports the results of work performed.

   - Whether practices conform to established standards.

Objective: Determine whether the board and senior management have established adequate procedures for ensuring compliance with applicable laws and regulations.

1. Determine the frequency of testing and reporting for compliance with laws and regulations.

   Consider:

   - Audit schedules, scopes, and reports.

   - Minutes of senior management and board committees.

   - The payment of any fines or liabilities arising from litigation against the institution or its employees.

2. Determine whether appropriate attention and follow-up are given to violations of laws and regulations.

   Consider:

   - The significance and frequency of the violations.
   - The willingness and ability to prevent reoccurrence.

Accounting, Information, and Communication Systems

Conclusion: The systems for accounting, information, and communication are (strong, satisfactory, weak).

Objective: Determine whether internal controls and information systems are appropriate and adequately tested and reviewed.

1. Assess the adequacy of accounting systems.

   Consider:

   - Whether accounting systems properly identify, assemble, analyze, classify, record, and report an institution's transactions in accordance with GAAP.

   - Whether the systems account for the assets and liabilities involved in transactions.

2. Assess the adequacy of information systems.

   Consider:

   - Type and extent of reports generated for operational, financial, managerial, and compliance-related activities.

   - Whether reports are sufficient to properly run and control the institution.

3. Assess the adequacy of communication systems.

   Consider:

   - Whether significant information is imparted throughout the institution (from the top down and from the bottom up in the organizational chain), ensuring that personnel understand:

     – Their roles in the control system.
     – How their activities relate to others.
     – Their accountability for the activities they conduct.

   - Whether information is imparted to external parties such as regulators, shareholders, and customers.

4. Assess the frequency and extent of verification of the accounting, information, and communication systems.

Consider:

- The frequency of testing given the level of risk and sophistication of the systems.
- The sufficiency of ongoing reviews of the systems' accuracy.
- The competency, knowledge, and independence of the personnel performing the testing.
- The sufficiency of contingency planning.

Self-assessment and Monitoring

Conclusion: The self-assessment and monitoring process is (strong, satisfactory, weak).

Objective: Determine whether senior management and the board provides appropriate oversight and attention to internal controls, control reviews, and audit findings.

1. Determine whether senior management and the board or board committee have reviewed actions taken by management to deal with material control weaknesses and verified that those actions are objective and adequate.

   Consider:

   - Minutes of appropriate meetings.
   - Audit or other control review reports and follow-up reports.

2. Determine the frequency and comprehensiveness of reports to the board or board committee and senior management.

   Consider:

   - Review of the minutes of appropriate meetings.
   - Whether the detail within the reports is sufficient.
   - Whether reports are presented in a timely manner to allow for resolution and appropriate action.

3. Determine the adequacy of the review of audit and other control functions by the audit or other appropriate board committee. Does the scope of their review consider the:

   - Selection of key personnel?
   - Approval of the overall scope of review activities (e.g., audit, loan coverage, etc.)?
   - Review of results?
   - Approval of the system of internal controls?
   - Periodic review of audit or other key control systems?

Objective: Determine whether audit or other control review findings, and management responses to those findings, are fully documented and tracked for adequate follow-up.

1. Assess the adequacy and independence of the audit or other control review function.

   Consider:

   - Results of the review of internal or external audit or other control review working papers.
   - Organizational structure and reporting lines.
   - The scope and frequency of audits or reviews for all lines of business.
   - Audit or control review reports, management responses, and follow-up reports.

2. Determine whether line management is held accountable for unsatisfactory or ineffective follow-up to control weaknesses.

3. Assess the adequacy of documentation detailing the coverage, findings, and follow-up of control weaknesses.

4. Determine whether management gives appropriate and timely attention to material control weaknesses once identified.

Objective: Determine the reliability of the institution's audit and control review functions through periodic and ongoing validation.

1. Validate, through transaction testing, the integrity of key control systems. Validation should ensure that the various control systems are covered by one of the following validation cycles:

    - For large banks, validate control systems annually for high-risk areas, and once every three years for low-risk areas.

    - For community banks, validate controls every supervisory cycle.

2. When in need of further guidance on validation testing, refer to procedures for specific banking activities in other booklets of the *Comptroller's Handbook*

Conclusions

1. Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. Cover the following subjects:

   - Quantity of risk assumed by the bank from violations of laws or regulations and nonconformance with established internal policies and procedures related to the internal control functions.
   - Quality of the bank's internal control processes to control risk in bank operations.
   - Adequacy of internal control policies, procedures, and programs.
   - Whether bank personnel conform with established policies and, if not, the causes and consequences of nonconformance.
   - Whether management and the board receive adequate information on the internal control function.
   - Audit or other control review report findings not acted upon by management, as well as any other concerns or recommendations resulting from the review of internal control functions.
   - Recommended corrective actions, if applicable, and management's commitments to same.

2. Determine the effect any identified internal control risks have on each risk category's aggregate risk and direction of risk. Examiners should refer to guidance provided by risk assessment programs for the OCC's large and community banks.

3. Determine, in consultation with the EIC, whether the internal control risks identified are significant enough to merit bringing them to the board's attention in the report of examination. If so, prepare items for inclusion under the heading "Matters Requiring Board Attention" (MRBA).

   - MRBA comments should cover practices that:
     - Deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed.
     - Result in substantive noncompliance with laws.

- MRBA comments should discuss:

  – Factors contributing to the problem.
  – Consequences of inaction.
  – Management's commitment to corrective action.
  – The time frame(s) and person(s) responsible for corrective action.

4. As appropriate, prepare an internal control comment for inclusion in the report of examination. The comment should discuss:

   - Adequacy of internal control policies, processes, personnel, systems, and overall internal control programs.

   - Significant problems that have not been corrected.

   - Any deficiencies or concerns reviewed with management, any corrective actions recommended by examiners, and management commitments to corrective actions.

5. Prepare a memorandum and update work programs with any information that will facilitate future examinations.

6. Update the OCC database and any applicable report of examination schedules or tables.

7. Organize and reference working papers in accordance with OCC guidance (PPM 5400-8).

Statutory and Regulatory Requirements

By law, national banks must adhere to certain requirements regarding internal controls. These requirements ensure that banks operate in a safe and sound manner, accurately prepare their financial statements, and comply with other banking laws and regulations.

Operational and Managerial Standards

In July 1995, the OCC issued 12 CFR 30 establishing operational and managerial standards for national banks. The subjects of certain of these standards are internal control and information systems. Appendix A to 12 CFR 30 states that a national bank should have internal control and information systems that are appropriate to the size of the bank and the nature, scope, and risk of its activities. According to the appendix, such systems should provide for:

- An organizational structure that establishes clear lines of authority and responsibility for monitoring adherence to prescribed policies;
- Effective risk assessment;
- Timely and accurate financial, operational, and regulatory reports;
- Adequate procedures to safeguard and manage assets; and
- Compliance with applicable laws and regulations.

When a national bank fails to meet these standards, the OCC may require it to submit a compliance plan to its supervisory office.

Annual Independent Audit and Reporting Requirements

12 CFR 363 on audits, related reports, and audit committees applies to national banks with $500 million or more in total assets. Under the regulation, these national banks must submit an annual report to their OCC supervisory office and the FDIC. The annual report must include:

- A management report containing:
  - A statement of management's responsibilities to prepare financial statements, establish and maintain an internal control system and procedures for financial reporting, and comply with safety and soundness laws concerning loans to insiders.
  - Management's assessment of the effectiveness of the bank's internal control system and procedures for financial reporting as of the end

of the fiscal year, and management's assessment of the bank's compliance with designated laws and regulations during the most recent fiscal year.

- A report by the independent public accountant attesting to management's assertions regarding internal control on financial reporting.

Federal Securities Laws

All national banks with a class of securities registered pursuant to the Securities Exchange Act of 1934 are required by 15 USC 78m to develop and maintain a system of internal accounting controls. These requirements help the Securities and Exchange Commission to oversee securities transactions and exchanges. Such controls should ensure that:

- Transactions are executed in accordance with management's general or specific authorization;

- Transactions are recorded as necessary to permit preparation of financial statements in conformance with generally accepted accounting principles or any other criteria applicable to such statements, and to maintain accountability for assets;

- Access to assets is permitted only in accordance with management's general or specific authorization; and

- Accounting records on assets are compared with the assets at reasonable intervals and appropriate action is taken to reconcile any differences.

Foreign Corrupt Practices Act

Laws	15 USC 78m

Independent Public Accountant Attestation

Laws	12 USC 1831s
Regulations	12 CFR 363

Information Systems

FFIEC Issuances	FFIEC IS Examination Handbook
OCC Issuances	OCC 96-39, "Data Communications Networks, Risks, and Control Systems"

Operational and Managerial Standards

Laws	12 USC 1831p-1
Regulations	12 CFR 30

Industry Reference Sources

AICPA Audit and Accounting Guide, "Banks and Savings Institutions."

AICPA Statement on Auditing Standards 55, "Consideration of the Internal Control Structure in a Financial Statement Audit."

AICPA Statement on Auditing Standards 70, "Reports on the Processing of Transactions by Servicing Organizations."

AICPA Statement on Auditing Standards 78, "Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55."

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control — Integrated Framework.* Vol. 1*, Executive Summary*. Vol. 2, *Framework*. Vol. 3, *Reporting to External Parties*. Vol. 4, *Evaluation Tools*.

Deloitte Touche Tohmatsu International, *Internal Audit in Leading Financial Institutions*.

Ernst & Young, *Evaluating Internal Control.* Three booklets: "A Guide for Management," "Assessment of the Control Environment: Documentation Supplement," and "Application Evaluations: Documentation Supplements."

The Institute of Internal Auditors, *Control Self-Assessment: Making the Choice*.